1.4. ПОЧЕМУ КОМИССИЯ В БИТКОИН-ТРАНЗАКЦИЯХ НАСТОЛЬКО МАЛА И КАК ОНА РАССЧИТЫВАЕТСЯ?

Козырь В.Ю. – старший инженер ЦЭМИ РАН, помощник оценщика

В статье рассмотрен принцип работы экосистемы сети Биткоин и формирование комиссии за транзакцию.

Введение

В традиционной экономике размер банковских транзакционных комиссий зависит от суммы транзакции и рассчитывается как доля от этой суммы. Однако цифровая экономика живет по другим «законам». Комиссия в сети Биткоин на первый взгляд кажется хаотичной, ведь условная транзакция на сумму 1000 BTC может иметь меньшую комиссию, чем транзакция на сумму 1 BTC. В качестве примера на рисунках ниже приведены две биткоин- транзакции в долларовом выражении с близкой по размеру комиссией и многократной разницей в сумме самой транзакции (рисунки 1 и 2).

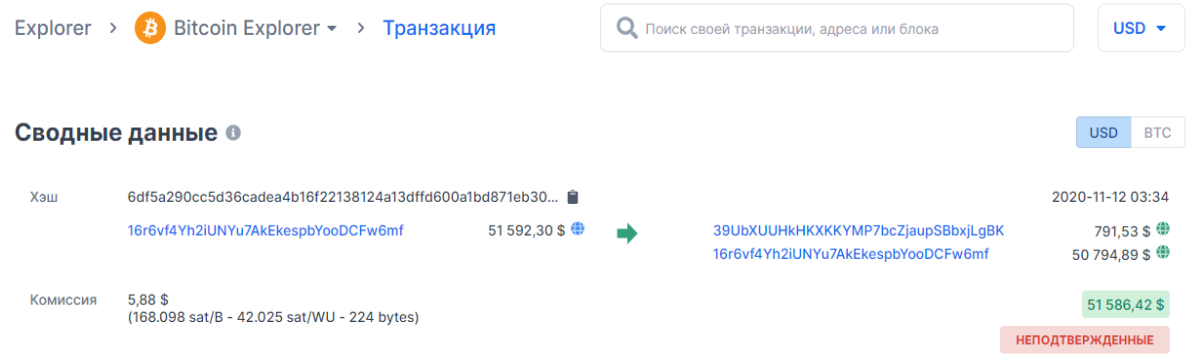

Рисунок 1. Сумма транзакции эквивалентна 51 586,42 $. Размер комиссии эквивалентен 5,88 $.

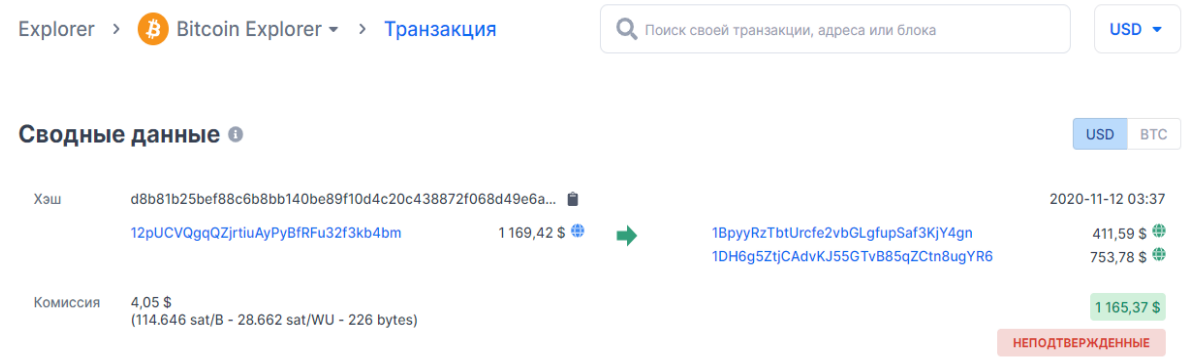

Рисунок 2. Сумма транзакции эквивалентна 1 165,37 $. Размер комиссии эквивалентен 4,05 $.

При этом есть множество примеров, когда транзакции в сети Биткоин, эквивалентные десяткам и даже сотням миллионов долларов, имели комиссионные издержки размером в несколько «баксов». В этой статье мы рассмотрим, как формируются такие комиссии, от чего зависит их размер, и кто их получает.

Как это работает

Биткоин сам по себе достаточно сложен в плане обработки транзакций. Упрощенно процесс обработки транзакций можно описать так: когда вы хотите отправить часть баланса кому-либо, то с вашего кошелька уходит не часть баланса, а вся сумма, разделенная на нового владельца с его долей (тем, что вы ему отправили) и сдачей на ваш адрес (тем, что осталось от баланса за вычетом комиссии транзакции). Весь этот процесс отправки, разделения и возврата «сдачи» происходит в рамках одного блока[1], одной транзакции. После подтверждения отправки вы сможете использовать «сдачу» для следующих своих транзакций.

[1] Блок – это файл, в который записываются данные о транзакциях. Каждый блок может содержать не более 1 Мб информации. Включение транзакции в блок происходит во время процесса майнинга.

Комиссия в сети Биткоин – это сбор, который владельцы биткоинов платят майнерам[2] за перевод средств на тот или иной адрес. Этот сбор не вычитается из суммы транзакции, а добавляется к ней. Поэтому на счету должно быть больше «монет», чем необходимо отправить.

Раньше комиссии взимались по другим правилам: если транзакция была достаточно маленькой или имела «приоритет», она могла быть бесплатной. Сегодня же все иначе, и комиссия требуется всегда. Исключение составляют транзакции по зачислению вознаграждения за майнинг и транзакции по взиманию самой комиссии, так как все это происходит в рамках одной операции.

Минимально возможный размер комиссии составляет 1 Сатоши[3] за байт. При этом размер комиссии может регулироваться самим отправителем. От размера выбранной комиссии зависит скорость обработки транзакции. В среднем на транзакцию может уходить до 1 часа, но в моменты пиковой нагрузки на сеть транзакции могут обрабатываться десятками часов и даже дней.

Комиссия формирует приоритет транзакции в очереди ожидания, называемой Мемпул (память майнера - Mempool[4]) (рисунок 3). Чем больше размер этой очереди, тем выше время ожидания подтверждения транзакции. И чтобы его сократить, придется увеличить размер комиссии.

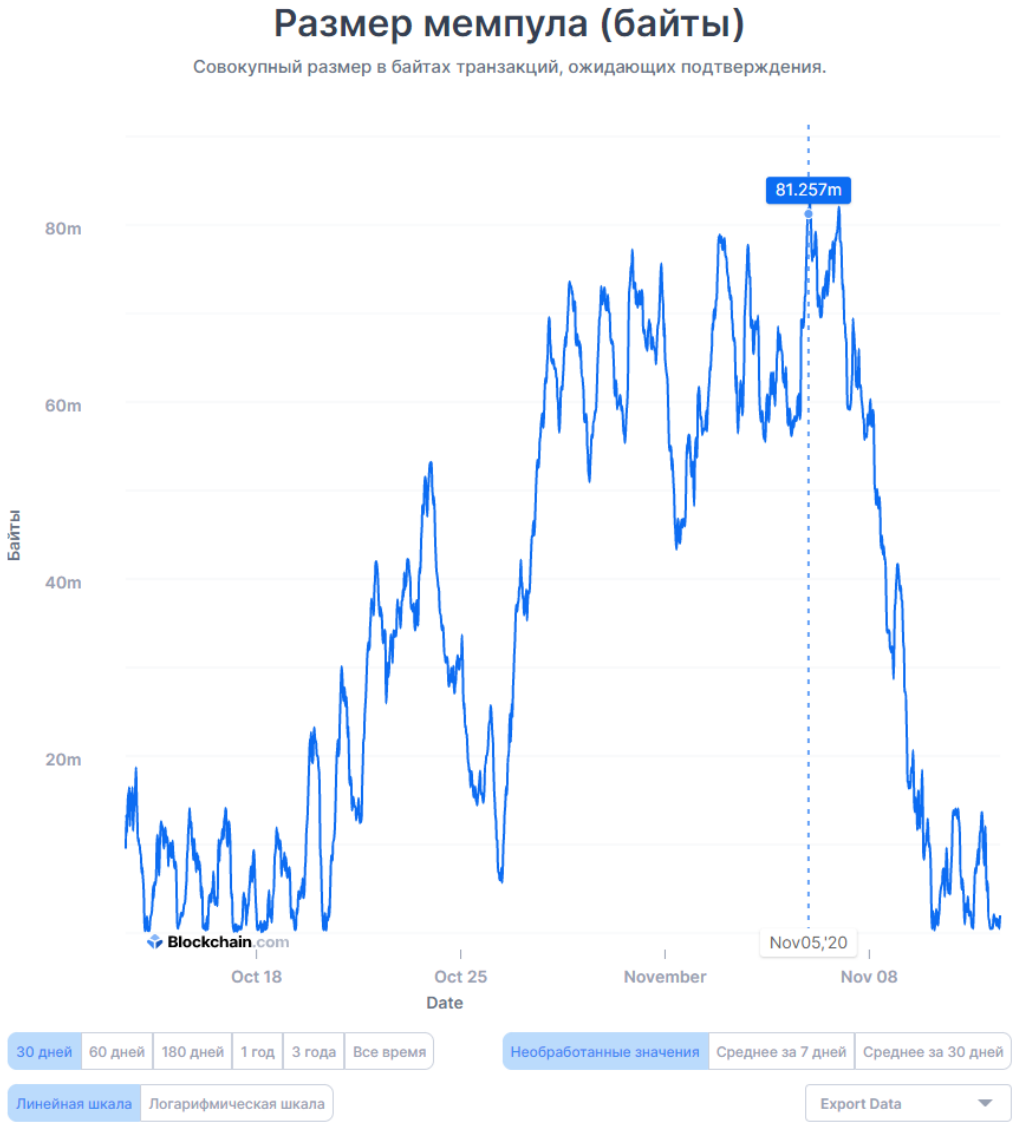

Рисунок 3. Размер очереди ожидания биткоин-транзакций

[2] Майнер – это компьютер, поддерживающий сеть Биткоин.

[3] Сатоши – это 10^{-8} биткоина. Минимальная единица этой криптовалюты, которая названа в честь основателя Bitcoin – Сатоши Накамото.

[4] Мемпул – это место, где все действующие транзакции ожидают подтверждения от сети Bitcoin. Большой размер мемпула указывает на больший сетевой трафик, что приводит к увеличению среднего времени подтверждения и более высоким комиссиям за приоритет. Размер мемпула является хорошим показателем для оценки продолжительности перегрузки.

Как видно из рисунка 3, размер мемпула постоянно меняется и практически не ограничен в размерах, если не считать ограничений размера самой сети, которая имеет гигантские масштабы.

Современные биткоин-кошельки для удобства предлагают два вида комиссии – Regular (обычные) и Priority (приоритетные). Эти комиссии имеют динамический характер и рассчитываются автоматически. Обычные комиссии ниже, но на подтверждение транзакции может уйти больше часа. Плата за приоритетность выше, но рассчитывается исходя из того, чтобы транзакция подтвердилась в течение одного часа. Хотя обычно это происходит за несколько минут.

Транзакция в сети Биткоин проводится по следующему алгоритму:

1. Пользователи инициируют платеж.
2. Транзакция отправляется в мемпул.
3. Приблизительно каждые 10 минут майнеры объединяют множество транзакций в блок.
4. Майнеры подтверждают новую транзакцию[5].
5. За свою работу в виде затраченных мощностей майнеры получают награду в форме эмитированных биткоинов и комиссии за транзакцию.
6. Блок добавляется в общую базу данных всех биткоин-транзакций – блокчейн сети Биткоин.
7. Изменения баланса отображаются на счетах участников транзакции.

Каждый блок содержит информацию о количестве сделок, их сумме и сумме уплаченной комиссии (рисунок 4).

Недавние блоки

Высота	Возраст	Сделки	Всего отправлено	Общие сборы	Размер блока (в байтах)
656587	2020-11-12T13: 02: 31.245Z	2,499	5 133,355 BTC	0,761 BTC	855 955
656586	2020-11-12T12: 59: 19.639Z	3110	50 002,202 BTC	1,533 BTC	921 203
656585	2020-11-12T12: 27: 11.324Z	2,453	26 007,335 BTC	0,791 BTC	856 087
656584	2020-11-12T12: 14: 14.748Z	2,408	2665,882 BTC	0,304 BTC	934 774
656583	2020-11-12T12: 11: 16.841Z	2387	1,000,78 BTC	0,284 BTC	907 385

Рисунок 4. Список недавних блоков[6].

В каждом блоке 30 000 байт выделены для транзакций с высочайшим приоритетом, они никак не зависят от комиссии. Затем в блок добавляются транзакции, которые имеют минимальную и выше комиссию. Чем выше комиссия, тем больше приоритет. Максимальный размер блока составляет 1 000 000 байт. Не вошедшие в состав блока транзакции остаются в памяти майнера (mempool) и могут быть включены в последующие блоки.

Расчет комиссии

Когда вы отправляете биткоин-перевод, формируется транзакция, состоящая из определенного количества символов. Каждый символ – это байт информации. А каждая транзакция – это программный код, который генерируется, учитывая то, откуда пришли биткоины и то, куда они отправляются. Чем больше адресов участвуют в транзакции – тем длиннее получается код.

В большинстве случаев[7] расчет размера транзакции производится по формуле:

148 * In + 34 * Out + 10,

где:

In – количество «входов»,

Out – количество «выходов».

```
143  Transaction.guessSize = function (nInputs, nOutputs) {
144    if (nInputs < 1 || nOutputs < 1) { return 0; }
145    return (nInputs * 148 + nOutputs * 34 + 10);
146  };
```

Рисунок 5. Фрагмент программного кода, отвечающий за расчет размера транзакции[8]

Приведем простой пример, без учета комиссии: вы получили 2 BTC от Миши и 5 BTC от Димы, а затем отправили 6 BTC Маше. При этом система списывает у вас все 7 BTC, 6 из которых переводит

[5] Включение в 1 блок = 1 подтверждение, когда таких подтверждений набирается 6 и выше транзакция считается подтвержденной. Такая функция была введена для защиты от повторной траты одних и тех же биткоинов.

[6] Источник: https://live.blockcypher.com/btc/

[7] При использовании стандартных Legacy-адресов.

[8] Данная функция взята из программного кода биткоин-кошелька Blockchain.info. Код находится в открытом доступе на Github и доступен по ссылке: https://clck.ru/RwGch

Маше, а оставшуюся «сдачу» переводит обратно вам. Следовательно, в этой транзакции участвует 4 адреса (Миша, Дима, Маша и Вы сами).

1. Каждый адрес, с которого получены средства (вход) — это + 148 байтов.
2. Каждый адрес, на который уходят средства (выход) — это + 34 байта.
3. Каждая транзакция занимает еще + 10 байтов, независимо от количества адресов, которые в ней участвуют.

Подставляем значения в вышеприведенную формулу и получаем размер транзакции 374 байта:

148 * 2 + 34 * 2 + 10 = 374.

Теперь, чтобы вычислить итоговый минимальный размер комиссии – умножаем размер транзакции (374 байта), на минимальную ставку комиссии 1 сатоши за байт. Получается, что для совершения этой транзакции нам необходимо заплатить 374 сатоши, или 0,00000374 BTC.

Для того, чтобы узнать оптимальный размер комиссии, можно воспользоваться информационным сервисом[9], который рассчитывает размер комиссии с учетом текущей загруженности сети:

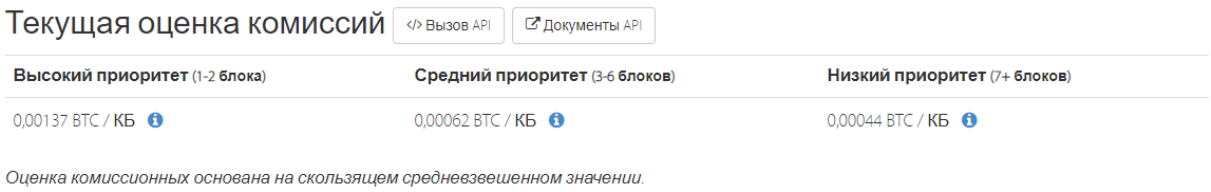

Рисунок 6. Комиссия с учетом текущей загруженности сети[10]

Рассчитаем размер комиссии для нашей транзакции, размером 374 байта:

1. Высокий приоритет: 0,00137 * 374 / 1000 = 0, 000512 BTC;[11]
2. Средний приоритет: 0,00062 * 374 / 1000 = 0, 000232 BTC;
3. Низкий приоритет: 0,00044 * 374 / 1000 = 0, 000165 BTC.

Как видно из полученных результатов, даже комиссия с низким приоритетом гораздо выше, чем минимально возможная. А значит, сеть находится под нагрузкой, и в случае с минимально возможной комиссией время ожидания подтверждения транзакции может исчисляться сутками.

Для того чтобы разгрузить сеть, снизить размер комиссии и время ожидания подтверждения транзакции, был изобретен протокол Segregated Witness (SegWit). Он позволил сократить вес транзакций в блоках сети Bitcoin за счет удаления из них подписей и выносе их в «дополнительные данные», с последующей индивидуальной обработкой.

В будущем новые SegWit-адреса полностью заменят Legacy-адреса. Причем это будет сделано автоматически во время транзакции. То есть вы делаете перевод со своего старого Legacy-адреса и получаете вашу «сдачу» уже на новый адрес с протоколом SegWit.

Кроме того, для снижения нагрузки на сеть Биткоин, а также времени ожидания подтверждения транзакции некоторые биткоин-кошельки, такие как Coinbase, стали проводить транзакционные операции внутри своей сети. При необходимости такие операции отправляются в глобальную сеть Биткоин, но уже с изначально высоким приоритетом и обрабатываются майнерами в первую очередь.

Заключение

Все транзакции внутри сети Биткоин обрабатываются поддерживающими эту сеть узлами – то есть майнерами.

Размер комиссии за транзакцию зависит не от суммы транзакции, а от размера этой транзакции в байтах и может определять ваш приоритет в очереди на подтверждение транзакции.

Также немалую роль в определении размера комиссии играет текущая загруженность сети. Ведь установив минимальную комиссию, вы рискуете зависнуть в ожидании подтверждения транзакции на целые дни и даже недели. Кроме того, на размер транзакции, и, следовательно, размер комиссии влияют используемые технологии (SegWit) и даже «хитрости» (Coinbase).

На данный момент сеть Биткоин не готова обслуживать большое количество транзакций, как это делают современные платежные системы, такие как Visa и MasterCard. Поэтому претендовать на звание платежной системы ей еще рано. Однако технологии не стоят на месте, и, возможно, новые решения смогут устранить эту проблему.

Литература

1. Andreas M. Autolopoulos. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. – Oreilly Media, 2014, URL:https://github.com/bitcoinbook/bitcoinbook

[9] https://live.blockcypher.com/btc/

[10] В скобках напротив приоритета (см. рисунок 5) указано в какой по очереди блок может попасть наша транзакция.

[11] Размер комиссии указан из расчета на 1 КБ, делим размер транзакции на 1000, чтобы перевести байты в килобайты.

2. Andreas M. Autolopoulos. Mastering Bitcoin: Programming the Open Blockchain. – Oreilly Media, 2017.
3. Nicola Atxei and Massimo Baronetti. A formal model of Bitcoin transactions. – 2017. URL: https://eprint.iacr.org/2017/1124.pdf
4. Satoshi Nakamoto Bitcoin: A Peer-to-Peer Electronic Cash System. – URL:https://bitcoin.org/bitcoin.pdf

Использованные ресурсы:
1. https://www.blockchain.com/
2. https://bitcoin.org/
3. http://cryptowiki.net/
4. https://bitinfocharts.com/
5. https://live.blockcypher.com/
6. https://ru.bitcoinwiki.org/
7. https://altwiki.ru/
8. https://bitinfocharts.com/ru/comparison/transactionfees-btc-eth.html
9. https://github.com/blockchain
10. https://clck.ru/RwGch

Использованные статьи:
1. https://clck.ru/RwGWd
2. https://clck.ru/RwGW9
3. https://clck.ru/RwGXE
4. https://clck.ru/RwGXk
5. https://clck.ru/RwGrm

Владислав Юрьевич Козырь – инженер ЦЭМИ РАН
(y_k65@mail.ru)

Ключевые слова
Биткоин[12], биткоин[13], BTC, блокчейн, майнер

***Vladislav Kozyr,* Why Bitcoin transaction fees are so low and how are they calculated?.**

Keywords
Bitcoin, bitcoin, BTC, blockchain, miner

DOI: 10.34706/DE-2020-03-04
JEL classification M 31 – Marketing

Abstract
The article discusses the principle of the Bitcoin network ecosystem and the formation of a transaction fee.

[12] Bitcoin или Биткоин (с большой буквы) – когда речь идет о технологии, сети, концепции.
[13] bitcoin или биткоин (с маленькой буквы) – когда идет речь о единице валюты.